

## ABSTRACT

REDUCING THE BOOT TIME OF A TCPA BASED COMPUTING SYSTEM  
WHEN THE CORE ROOT OF TRUST MEASUREMENT IS EMBEDDED IN THE  
BOOT BLOCK CODE

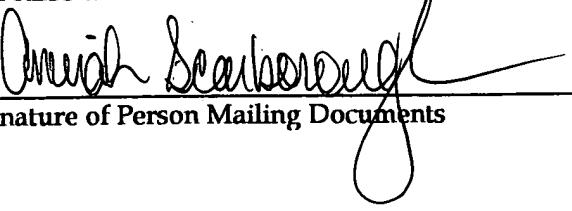
5           A method, computer program product and system for reducing the boot time  
of a TCPA based computing system. A flash memory in the TCPA based computing  
system may include a register comprising bits configured to indicate whether the  
segments of the flash memory have been updated. The flash memory may further  
include a table configured to store measurements of the segments of the flash  
10          memory. The flash memory may further include a boot block code that includes a  
Core Root of Trust for Measurement (CRTM). The CRTM may read the bits in the  
register to determine if any of the segments of the flash memory have been updated.  
The CRTM may further obtain the measurement values in the table for those  
segments that store the POST BIOS code that have not been updated thereby saving  
15          time from measuring the POST BIOS code and consequently reducing the boot time.

AUS  
7036CERTIFICATE OF MAILING UNDER 37 CFR§ 1.10

I hereby certify that this correspondence is being deposited with the  
United States Postal Service as Express Mail in an envelope addressed to  
the Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450  
on

November 13, 2003.

EXPRESS MAIL LABEL: EV 331727587 US

  
\_\_\_\_\_  
Signature of Person Mailing Documents